On ℓ^3-divisibility of class numbers of ℓ-cyclic extensions(Algebraic Number Theory)

NAITO, Hirotada

数理解析研究所講究録
603巻 1987年 87-92

On ℓ^3-divisibility of class numbers of ℓ-cyclic extensions

by Hirotada NAITO
内藤浩忠

The Faculty of Education
Kagawa University
Takamatsu, JAPAN

§ 1. Introduction.

In this talk, we consider a problem of the divisibility of class numbers of algebraic number fields of finite degree. Many people have studied the following problem:

Are there infinitely many algebraic number fields k satisfying some prescribed conditions whose class numbers are divisible by a given integer n?

Kuroda[7] studied the case that fields k are imaginary quadratic fields in which a finite number of prescribed primes are ramified.

Yamamoto[11] studied the case that fields k are real quadratic fields.

Uchida[10] studied the case that fields k are cyclic extensions over the rational number fields Q of degree 3.

Azuhata and Ichimura[1] studied the case that fields k have r_1 real places and r_2 imaginary places ($r_2 \geq 1$).

Nakano[9] generalized the above result to the case including $r_2=0$.

Further references are found in Diaz y Diaz[3].

For a special class of quadratic number fields we know the following theorem.

THEOREM (Kaplan[6] and Yamamoto[12]) Let $p\equiv 3 \pmod 4$ be the fixed prime. Let $q\equiv 1 \pmod 4$ be the prime. Then the following properties are equivalent:

(i) The class number of $Q(\sqrt{-pq})$ is divisible by 8.

(ii) The prime q is completely decomposed in K_8/Q, where $K_8=Q(\sqrt{-1},\sqrt[4]{p})$.

By Tchebotarev's density theorem we see that the density of the set consisting of the primes q with the above property (ii) is 1/8. Therefore we may say that the density of $Q(\sqrt{-pq})$ whose class numbers are divisible by 8 is 1/8 for the fixed prime p. Cohn[2] called such a field K_8 the governing field and studied some types of quadratic fields.

In this talk, we investigate the ℓ^3-divisibility of the cyclic extensions of degree ℓ, where ℓ is an odd prime number. Let p be the fixed prime such that $p\equiv 1 (\mathrm{mod}\ \ell)$ or $p=\ell$. Let $q\equiv 1 \pmod{\ell}$ be a prime. We denote by L_p the cyclic extension over the rational number field Q of degree ℓ where only the prime p is ramified. We denote by L_i $(1\leqq i\leqq \ell-1)$ the cyclic extensions over Q of degree ℓ where only both of the primes p and q are ramified. The class number of L_p is prime to ℓ and the index of the group of circular units of L_p in the unit group E of L_p is also prime to ℓ. Let ξ_1 and ξ_2 be circular units of L_p such that the images of the subgroups $\langle\xi_1\rangle$ and $\langle\xi_1,\xi_2\rangle$ in E/E^ℓ are invariant under the action of the Galois group of L_p/Q. We put $\mathcal{L}_p^2=L_p(\zeta_\ell,\sqrt[\ell]{\xi_1})$ and $\mathcal{L}_p^3=L_p(\zeta_\ell,\sqrt[\ell]{\xi_1},\sqrt[\ell]{\xi_2})$, where ζ_ℓ is a primitive ℓ-th root of unity. Then we get:

THEOREM. For $r=2$ or 3, the following properties are equivalent:

(i) The class number of L_i is divisible by ℓ^r for some $1\leqq i\leqq \ell-1$.

(ii) The class number of L_i is divisible by ℓ^r for any $1\leqq i\leqq \ell-1$.

(iii) The prime q is completely decomposed in $\mathcal{L}_p^r/Q$.

REMARK 1. For $r=2$, this is a result of Inaba[4], c.f. also Gras[5]. In these papers it is shown that the property (i) is equivalent to the property $\left(\frac{q}{p}\right)_\ell=\left(\frac{p}{q}\right)_\ell=1$, where $\left(\frac{*}{*}\right)_\ell$ is the ℓ-th power residue symbol. We get $\mathcal{L}_p^2=L_p(\zeta_\ell,\sqrt[\ell]{p})$ because of $\xi_1=p\alpha^\ell$ for some $\alpha\in L_p$. Thus we see that (i) and (ii) are equivalent.

REMARK 2. If the class number of L_i is divisible by 3^3, the ideal class group of L_i has an element of order 3^2 for $\ell=3$.

§ 2. The Proof.

We denote by $(Z/mZ)^{\oplus s}$ the direct sum of s cyclic groups of order m. We see by class field theory that the property (iii) in Theorem 4 is equivalent to the following

(iii)′ L_p has a $(Z/\ell Z)^{\oplus r}$-extension with conductor q.

At first we explain the case of $r=2$. Let H_c be the unramified $(Z/\ell Z)^{\oplus 2}$-extension over L_i such that H_c/Q is a Galois extension. Then H_c/L_j $(j \neq i)$ is an unramified $(Z/\ell Z)^{\oplus 2}$-extension. Moreover H_c/L_p is a $(Z/\ell Z)^{\oplus 2}$-extension with conductor q.

Next we explain the case of $r=3$. We see by Proposition VI.6. in Gras[4] that the properties (i) and (ii) are equivalent.

We assume (ii). Let H_i/L_i be the unramified extension whose Galois group is isomorphic to $(Z/\ell Z)^{\oplus 3}$ for $\ell \geq 5$ or to $(Z/3^2Z) \oplus (Z/3Z)$ for $\ell=3$ such that H_i/Q is a Galois extension. Let H be the compositum of H_i $(1 \leq i \leq \ell-1)$. We see by the computation of the Galois group H/L_p that H contains the $(Z/\ell Z)^{\oplus 3}$-extension H_p/L_p with conductor q. Thus we get (iii)′.

We assume (iii)′. Let H_p/L_p be the $(Z/\ell Z)^{\oplus 3}$-extension with conductor q. Let H_c/L_p be the $(Z/\ell Z)^{\oplus 2}$-extension in H_p such that H_c is a Galois extension over Q. Let $\mathfrak{P}$ be the prime ideal of L_p lying over p. The prime ideal $\mathfrak{P}$ is completely decomposed in H_c/L_p, because $\mathfrak{P}$ is invariant under the action of the Galois group of L_p/Q. Let $\mathfrak{P}_i$ be the prime ideal of L_i lying over p. We see that $\mathfrak{P}_i$ is completely decomposed in H_c/L_i. We see that H_c/L_i is an unramified $(Z/\ell Z)^{\oplus 2}$-extension. As $\mathfrak{P}_i$ is an element of genus group of L_i, we see by class field theory that L_i has an unramified abelian extension of degree ℓ^3. Thus we get (i).

REFERENCES.

[1] T. Azuhata and H. Ichimura : On the divisibility problem of the class numbers of algebraic number fields, J. Fac. Sci. Univ. Tokyo 30 (1984), 579-585.

[2] H. Cohn : Introduction to the construction of class fields, Cambridge Univ. Press, 1985.

[3] F. Diaz y Diaz : Sur le 3-rang des corps quadratique, Publ. Math. d'Orsay, N°78-11 (1978).

[4] G. Gras : Sur les ℓ-classes d'idéaux dans les extensions cycliques relatives de degre premier ℓ, Ann. Inst. Fourier, Grenoble 23.3(1973),1-48, 23.4(1973),1-44.

[5] E. Inaba : Über die Struktur der ℓ-Klassengruppe zyklischer Zahlkorper vom Primzahlgrad ℓ, J. Fac.Sci. Univ. Tokyo 4 (1940), 61-115.

[6] P. Kaplan : Divisibilité par 8 du nomble des classes des corps quadratiques dont le 2-groupe des classes est cycliques, et reciprocité biquadratique, J. Math. Soc. Japan 25 (1973), 596-608.

[7] S.-N. Kuroda : On the class number of imaginary quadratic number fields, Proc. Japan Acad. 40 (1964), 365-367.

[8] H. Naito : Some results on class numbers and unramified extensions of algebraic number fields, the 19th Taniguchi Symposium (1986).

[9] S. Nakano : On ideal class group of algebraic number fields, J. Reine Angew. Math. 358 (1985), 61-75.

[10] K. Uchida : Class numbers of cubic cyclic fields, J. Math. Soc. Japan 26 (1974), 447-453.

[11] Y. Yamamoto : On unramified Galois extensions of quadratic number fields, Osaka J. Math. 7 (1970), 57-76.

[12] Y. Yamamoto : Divisibility by 16 of class number of quadratic fields whose 2-class groups are cyclic, Osaka J. Math. 21 (1984), 1-22.